Privacy-protection Technologies for Secure Utilization of Sensor Data

● Tetsuya Izu ● Koichi Ito ● Hiroshi Tsuda ● Kenichi Abiru ● Takao Ogura

As the number of scenarios for utilizing sensor data such as household data from intelligent appliances and location information obtained from automobiles increases, social issues are arising, such as leakage of private information from sensor data. Fujitsu Laboratories has developed two privacy-protection technologies that provide total protection for such sensor data, from its collection to utilization of the results of its analysis. One, partial decryption technology, enables parts of the data to be masked while still encrypted, so other data can be substituted or the encryption key can be changed. The other, anonymous access technology, enables people to obtain the analysis results for their own data from a utilization service without providing their ID. These technologies give people appropriate control of their sensor-collected private information while also enabling them to use external analysis services anonymously. This article describes these technologies.

1. Introduction

Utilization of big data and other data sources has become the latest business model, and an increasing number of applications are now available for analyzing this data without disclosing personal information. In line with this, laws and guidelines are being implemented in an effort to increase society's acceptance of such applications, and technologies are being developed that protect privacy while maintaining utility for such purposes as anonymization and secure data mining. As an example, a decision by the Japanese cabinet in November 2012 resulted in a program to accelerate revitalization in Japan, including a study to create guidelines for anonymization and data utilization.

The scope of data being utilized is expanding to include household and presence data collected by intelligent appliances, location information from Global Positioning System (GPS) devices, images from surveillance cameras, management data from smart meters, and other sensor data. Previously, only limited privacy protection was given to sensor data, even data that included customer IDs, subscription data, and large amounts of other information linked to individuals. This is changing, as exemplified by the strengthening of data protection in the European Union (EU), which, in January 2012, mandated that EU residents must be able to maintain control of their private data even after it has been collected and stored by providers. For example, individuals must have the right to have their personal data deleted from a provider's database upon request. Regulations related to use of private data are becoming stricter globally, and similar regulations are expected to be imposed on sensor data. Accordingly, there is need for technologies that protect privacy while enabling sensor data to still be used effectively.[1)]

Fujitsu Laboratories has already developed and verified an anonymization technology for safely utilizing confidential data stored in the cloud.[2)] We have now extended this technology to protecting privacy when gathering and utilizing sensor data.[3)] This article describes the new technologies and the technical issues that needed to be resolved.

2. Technical issues

Sensor data includes information that can be used to identify individuals, such as customer IDs, and private information, such as addresses. For example, by associating various types of data such as home gateway data, smartphone location data, and blog or other social network data, one could identify the movements

and location of an individual. This raises the possibility of a variety of dangers such as burglary while the individual is not at home.

A mechanism is thus needed that enables private information in sensor data to be used while eliminating dangers such as these, and society must be convinced that such information can be used safely. Such a mechanism would enable people to control their private information. For example, they could mask out or replace parts of the data with other data so that service providers would receive only the data needed for providing the service.

Conventional encryption technology such as SSL communication protects data on a communication channel, but the data is decrypted at the receiving end, thereby revealing the original data. This means that privacy is not adequately protected. The financial industry uses tokenization technology to replace credit card and other ID data with different data. However, the need to tokenize the same data for each service provider individually and to use different encryption keys for each provider is troublesome.

3. Developed technologies

The two technologies developed to resolve the issues described in the previous section continuously protect sensor data by encryption from when it is collected until when it is used and enable it to be utilized safely, as illustrated in **Figure 1**.

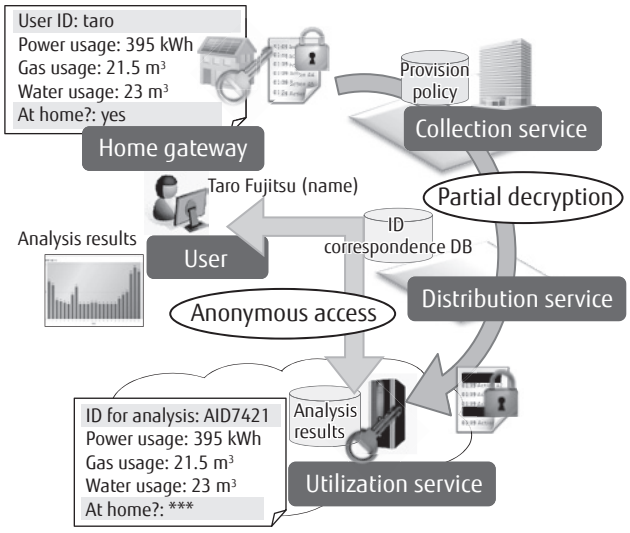

Figure 1
Potential use of developed technologies.

1) Partial decryption technology

The partial decryption technology enables parts of the sensor data to be masked and enables the data or encryption key to be changed while the data remains encrypted. When applied to transmission of data from a home gateway (Figure 1), all necessary processing, from when the data is sent from the gateway until it arrives at the utilization service, is done with the encryption intact. To control his/her data, a person simply configures the utilization service's provision policy (how the data is to be converted) beforehand. The conversion can include masking-out parts of the sensor data, converting the ID to a different ID for analysis purposes, and changing to a different encryption key for a service (**Figure 2**). The data is not decrypted from the time it leaves the home gateway until it arrives at the utilization service, so there is no possibility of leakage in transit. This means that privacy is completely protected. Data masking and key conversion can be done without decrypting the data, so protection and utility are both maintained.

The partial decryption technology is implemented using a shared, commutative encryption key.[3), 4)]

2) Anonymous access technology

The anonymous access technology enables customers to obtain the results of analysis from a utilization service without disclosing their own ID. One example of such a service is the provision of day-to-day power consumption graphs and power-saving advice based on power consumption data gathered from smart meters. There are various problems with implementing such a service in a form where the customer logs directly into the service to obtain analysis results. For example, the service would know in what time periods the customer is using power and could identify periods when the customer is likely to be away from home. The service must also maintain and protect customer accounts and personal information.

With anonymous access technology, customers can obtain their individual analysis results by accessing the utilization service anonymously through an anonymous access application (**Figure 3**). When the utilization service receives a request for analysis results from the anonymous access application, it issues an access ticket (like the numbered tickets dispensed in banks and other commercial places to customers awaiting service). The customer then logs into a distribution

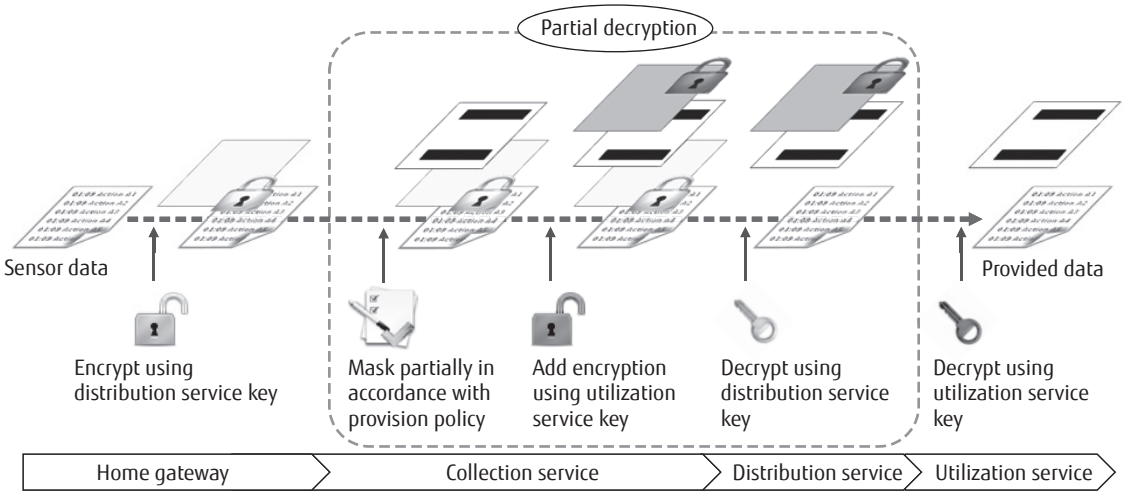

Figure 2
Partial decryption technology overview.

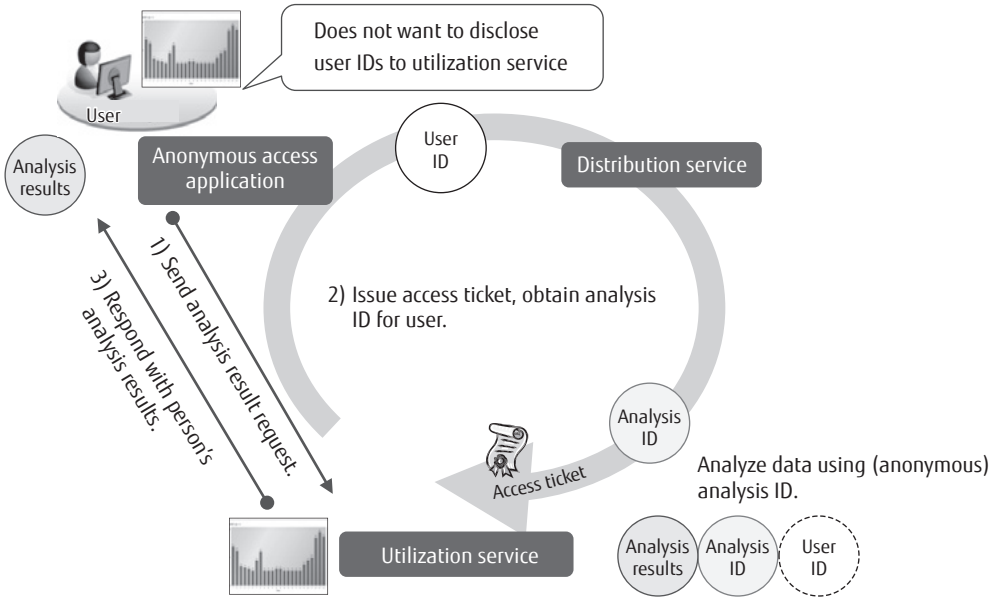

Figure 3
Anonymous access technology overview.

service using his/her ID and enters the access ticket information. The distribution service substitutes an analysis ID for the customer ID and then sends the analysis ID to the utilization service together with the access ticket. The utilization service performs the data analysis using the analysis ID and returns the result to the customer to whom it issued the ticket.

The above operations do not disclose the customer's ID to the utilization service, avoiding such problems as identifying when customers are not at home. Another benefit is that the utilization service is not required to manage unnecessary personal information.

4. Conclusion

This article has described two technologies newly developed by Fujitsu Laboratories for protecting private information in sensor data. The ability to control one's

private information is becoming more important, and privacy regulations such as those implemented in the EU will become more common. With the technologies described here, a person can safely provide sensor data containing private information to a collection service, and the data can subsequently be entrusted to various utilization services because the person continues to control the content and the data remains in encrypted form. Applying these technologies to smart meters, for example, will enable customers to compare their power-use tendencies with the average in their region and to optimize power use within their house without disclosing which house is theirs. Applying them to vehicle operations, as another example, will enable drivers to analyze dangerous driving areas without being identified.

Future plans include combining these technologies with information gateway technology,[5] verifying them by using location data, classified data, and other real data, and later, using them to link cloud infrastructures and for network services.

References

1) Fujitsu Technology and Service Vision. *http://www.fujitsu.com/global/vision/paper/*
2) H. Tsuda et al.: Inter-Cloud Data Security for Secure Cloud-Based Business Collaborations. *Fujitsu Sci. Tech. J.*, Vol. 48, No. 2, pp. 169–176 (2012).
3) Fujitsu: Fujitsu Develops Novel Technologies to Protect Sensor Data Privacy, from Collection to Utilization, October 22, 2012. *http://www.fujitsu.com/global/news/pr/archives/month/2012/20121022-01.html*
4) S. Idani et al.: A Privacy Protection System Applied to Utilization of Sensor Data. Computer Security Symposium 2012, October 2012 (in Japanese).
5) T. Izu et al.: Utilization of Sensor Data with Consideration for Protecting Privacy. Computer Security Symposium 2012, October 2012 (in Japanese).

Tetsuya Izu
Fujitsu Laboratories Ltd.
Mr. Izu is engaged in R&D on information security technologies.

Kenichi Abiru
Fujitsu Laboratories Ltd.
Mr. Abiru is engaged in R&D on network service provision technologies.

Koichi Ito
Fujitsu Laboratories Ltd.
Mr. Ito is engaged in R&D on data anonymization technologies.

Takao Ogura
Fujitsu Laboratories Ltd.
Mr. Ogura is engaged in R&D on service-linking technologies.

Hiroshi Tsuda
Fujitsu Laboratories Ltd.
Mr. Tsuda is engaged in R&D on data-centric security technologies.